

selections. This problem can result in “vote flipping” between candidates. DRE touchscreens can also be misprogrammed – deliberately or accidentally – in ways that can cause the votes not to track accurately. Logic and Accuracy (L & A testing) in advance of elections is supposed to catch and provide the opportunity to correct such errors before voters cast their ballots. But few election jurisdictions use the depth and scope of L & A testing required to assure that their DRE systems have not been misprogrammed or have “rogue code” planted on them. Malware and code designed to mis-record voters’ choices by changing votes to count for other candidates can be designed to activate only at a certain time after the L & A testing, and there are many other ways for cheating code to avoid being detected by L&A tests.

13. The DREs cannot function without an EMS configuring the ballot and generating the “instructions” that the DRE will use for presenting the ballot to the voter and recording the cast votes. Hence, the EMS and DRE vulnerabilities – both as to security and reliability -- are interrelated and impact one another.

14. As examples of how normal functioning of a poorly designed EMS can lead to the vote tabulation database “dumping” data – i.e., votes -- or “corrupting” that data, I would submit the experience of Cuyahoga County, Ohio. Because I served as the Project Director of the Public Monitor of Cuyahoga Election Reform, and had convened a technical team with access to tabulation records, we were able to publicly document that in the May 2006 primary, the GEMS database grew beyond the capacity that software could handle. Concretely, this meant that as DRE vote media and the scanned absentee ballot batches were uploaded to the GEMS server, GEMS covertly – without notice to officials-- dumped some of that data because its Microsoft JET / Access database foundation was not able to manage that amount of data. As a result, hundreds of votes in one county alone were not recorded and recounts determined that some previously announced winners actually had not won.

15. In the November general election of 2006, while preparing for the election and then on election night during the tabulations, the GEMS servers were repeatedly crashing. As Monitor, we staffed the tabulation server room and noted each time the server crashed; the security plan also required that an official record be made of each and every server crash, with its time and operator input when it occurred. Because we knew that servers crashing during tabulations could cause data corruption, we sought a forensic review of the database to ascertain whether vote data integrity had been preserved. We documented a number of indicators of data corruption, including database table element entries that missed their date/time stamps of when the information was entered; other tabulation entries' date/time stamps were marked "January 1, 1970," which is the epoch (zero- point) of UNIX time—rather than carrying the 2006 date and time. Finally, vote totals in two separate database tables held different values for the candidates' results, differing by hundreds of votes.

A Forensic Evaluation of the DREs Is the Only Way to Determine the Accuracy of the Vote

16. Given (a) the multiple available pathways for inserting malware or code that can cause vote flipping or miscounts; (b) the clear existence and motivation of numerous skilled and motivated hackers, including from nation-state adversaries; (c) the unreliability of the systems owing to their age and defective software designs, and (d) repeated crashing during pre-election and election tabulations, a recount that includes a forensics assessment of the EMS and at least a random selection of the DREs and associated components is necessary to ascertain whether the reported tallies are accurate.

17. Voting system experts who have no financial relationship to the vendors or their contracts, and who have developed expertise in these systems deployed in the Commonwealth can efficiently conduct forensics reviews in a targeted manner, focusing on the main frailties in these systems. For instance, in one 2-hour session in Cuyahoga County, one Monitor staff database examiner was able to document all the irregularities mentioned in paragraph 15,

supra. While most forensics assessments would not proceed this quickly, and investigating and correcting for the anomalies consumed some additional time, valuable information can be obtained in a matter of hours regarding whether the system performed as expected and required. . Forensics reviews are the only means to check whether all these functions are performed accurately for all-electronic DRE systems.

18. One of the additional values of an independent forensics review is that it allows the public and public authorities to obtain essential information relevant to whether and when they choose to replace the dilapidated voting systems. In Cuyahoga County, for instance, the officials made a decision to replace the GEMS-and-DRE system because it proved to be too unreliable and difficult to manage in a secure manner. In barely 1.5 years after our reports documenting these operational and the software architectural issues (that the vendor had hidden and that could not be fixed without a wholesale re-architecting of the software), Cuyahoga County chose to replace its voting system with a more reliable and accurate option.

19. Although I have personally listened to fears of election and other public officials that they will be accused of wrongdoing, or that the public will blame them personally for any problems that are discovered in a forensics review of election systems, or that the voting public will refuse to participate in voting if they learn of technical and other deficiencies in their election equipment, I would like to relate what occurred in Cuyahoga County. The May 2006 Federal primary election vote tally reports proved to be unreliable and inaccurate, in at least some races, and serious public questions were raised about the adequacy of the voting technologies. Instead of a superficial fix, our County's appointed independent investigatory team endeavored to figure out everything that had gone wrong, technically and managerially, and to disclose everything in public reports. We sought to assure the public that their voting rights were protected and that their choices would be accurately recorded and tabulated at least in future elections. We asked for the public's participation via public hearings on their

experiences and concerns, and retooled poll worker recruitment and training to ensure that fewer errors could occur at the polls. The public responded vigorously, attending standing room only public hearings and producing a large number of new volunteers to work as poll worker and in other roles. That fall, for the general election, our voting participation rates rose instead of falling and we had scores of new citizens involved in the election system in a variety of roles, all proving that transparency on voting problems can produce public energy and dedication to participate as well as help improve the election system.

20. As a voting systems and election administration specialist, and as cyber risk expert, I am concerned that hackers and other miscreants have learned that Pennsylvania has erected a series of legal obstacles that generally inhibit checking into the integrity of county election tabulations. Thinking from the security perspective, this legal cover basically provides a neon sign to motivated hackers both domestically and abroad, saying "*Come Hack Here; we won't be checking.*" Hackers seek valuable and preferably unprotected targets, and those who have been documented by Federal authorities to have interfered in this election cycle would have been highly motivated to try to probe and impact Pennsylvania's systems. As an election management and security specialist, I recommend that Pennsylvania clearly establish that its elections are not open to any motivated hacker and that the Commonwealth assures that accurate voting tallies are generated without incursion by unauthorized others.

This affidavit was executed on the 2nd day of December, 2016, in Cleveland, Ohio.


S. Candice Hoke

Sworn before me this 2nd day of December, 2016.


Notary Public

My Commission expires:

KENNETH J. KOWALSKI, Atty.
NOTARY PUBLIC • STATE OF OHIO
My commission has no expiration date
Section 147.03 O.R.C.

AFFIDAVIT OF MATTHEW A. BISHOP

I, Matthew A. Bishop, duly sworn, depose and say the following under penalty of perjury:

1. My name is Matthew Bishop. I am a co-director of the Computer Security Laboratory and a Professor of Computer Science at the University of California at Davis.

2. I received a Master of Arts degree in Mathematics from the University of California at Berkeley and a Master of Science and Ph.D. in Computer Science, both from Purdue University. I have worked as a systems programmer at Megatest Corp., a research scientist at the Research Institute for Advanced Computer Science, and as a faculty member in the Department of Mathematics and Computer Science at Dartmouth College and in the Department of Computer Science at the University of California at Davis, where I am now a full professor.

3. As a computer security researcher, I have devoted a major portion of my research on the security and accuracy of electronic voting systems, as well as modeling the procedures and processes with which an election is conducted. Here, my use of the term "voting systems" includes the central software system that is used to create the ballots and that aggregates and records the votes in a database before reporting the election tallies (often called the "EMS" or election management system); the direct recording electronic (DRE) voting devices that present electronic ballots to voters for their choices to be recorded; the DRE memory media that records the votes; the optical scanners used at some polls to read voter-marked paper ballots; the optical scanners used at a central location (for tabulating absentee ballots and for re-tabulating in the

official canvass the polling locations' op scan ballots); and any other module or component that is attached to or integrates with the EMS or voting devices to conduct the election.

4. I have been an active researcher in voting system security, examining software and hardware, operational usability, and election equipment forensics for over twelve years. In addition to scholarly research and numerous publications on voting systems security and forensics, and working directly with election officials who seek to improve their election security and other processes, my field experience with e-voting systems includes assessing the state of electronic voting systems before purchase (California), penetration testing of Diebold TS DRE systems (Maryland), a post-election forensics evaluation in a contested election (Florida, on the ES&S iVotronic, a model I understand to have been used in Allegheny County precincts in 2016), and co-leading a comprehensive study of the security and accuracy of voting system certified for use in California, undertaken for the California Secretary of State in the "Top to Bottom Review."

5. The California Secretary of State's charge to the Top-to-Bottom Review technical team asked whether "the systems currently certified should be left alone, or specific procedures required to provide additional protections for their use, or the machines simply decertified and banned from use" (Overview of Red Team Reports, §2.0, p. 1). I led the the "red team" penetration tests, and had access to the work of the other teams, including the source code reviews. The summary Red Team Report given to the Secretary concluded that "the security mechanisms [manufacturers had] provided for all systems analyzed *were inadequate to ensure accuracy and integrity of the election results* and of the systems that provide those results" (Overview of Red Team Reports, §6.4, p. 11; emphasis added). The systems analyzed included the Diebold GEMS 1.18.24/AccuVote, The Diebold Accuvote-TSX with AccuView Printer Module and Ballot Station Firmware version 4.6.4, the Hart Intercivic System 6.2.1 including the

eSlate/DAU version 4.2.13 and the eScan version 1.3.14, and the Sequoia WinEDS version 3.1.012/Edge/Insight/400-C.

6. From my review of information on the web about Pennsylvania's voting systems deployed in 2016, it appears that the California systems I studied in depth in the Top to Bottom Review, in the Maryland penetration tests, and in Florida's Congressional 13 race, all overlap significantly with those that Pennsylvania deployed in 2016.¹

DREs Are Unreliable and Vulnerable to Interference

7. Voting system security experts, including myself, have documented many vulnerabilities that can offer myriad covert opportunities for a motivated attacker to tamper with Pennsylvania's voting systems and ultimately cause the election tallies to fail to reflect the voters' choices.

8. "Hacking" or attacking the system is not the only type of problem with voting systems that can lead to inaccurate results. The accuracy of the election data, and specifically the electoral results, can be marred—sometimes significantly—simply because the software was not designed with the application of appropriate safeguards, coding principles, or database designs. These are some of the many types of software problems that have been documented in peer-reviewed scientific studies as well as in reviews of voting systems by others and myself.

9. As an example of an issue that speaks to the accuracy and integrity of the (formerly Diebold) GEMS software that is used to aggregate votes from e-voting systems and scanners and then tabulation and report results, all versions of the GEMS software that I have examined rely on the Microsoft Access database, which is built on top of software called the "JET engine." For the latest version of Microsoft Access, Access 2016, the maximum table size

¹ See for example <http://www.dos.pa.gov/VotingElections/OtherServicesEvents/Pages/Voting-Systems.aspx#.VIhhucIRqPI>

is 2 GB of data; extending this requires using multiple database files linked together. A database can hold no more than 32,768 objects, which in the context of an election would be ballots or votes.² These limits also hold in earlier versions of Microsoft Access, for example Access 2007³ and Access 2010.⁴ It is unclear what will happen if these data limits are exceeded. In the world of software, this is called “undefined behavior” and in elections, this uncertainty could result in inaccurate tabulations. As an example, on some computers,⁵ adding $65535 + 65535$ produces 65534, not 131,070 because the behavior of adding the two numbers exceeds the maximum number that the computer can store.

10. The software in the voting systems that I have personally studied have numerous flaws, including the addition flaw above. Some of these flaws could lead to incorrect recording of votes, or incorrect vote totals. These outcomes could occur in the absence of attacks.

11. There is considerable basis for doubting whether these voting systems are accurate and robust enough to produce trustworthy, accurate electoral tallies in general elections. We found that the systems used in California were not, as of the summer of 2007, despite having been certified to meet the requisite e-voting standards. Without access to the source code and to the systems themselves, it is impossible to know whether these problems, or other problems related to the accuracy and integrity of the systems, exist.

A Post-election Forensic Evaluations Is Necessary

12. The goal of a forensic examination of e-voting systems is to determine whether problems occurred that affected the accuracy and integrity of the system(s) and data in question.

² See *Access 2016 Specifications* at <https://support.office.com/en-us/article/Access-2016-specifications-0cf3c66f-9cf2-4e32-9568-98c1025bb47c>

³ See *Access 2007 Specifications* at <https://support.office.com/en-US/article/Access-2007-specifications-2EEDF198-6B27-4DC5-AE07-3E1FBA6D6C96>

⁴ See *Access 2010 Specifications* at <https://support.office.com/en-US/article/Access-2010-specifications-1E521481-7F9A-46F7-8ED9-EA9DFF1FA854>

⁵ Specifically, computers with 16 bit integers.

This type of examination leads either to an increased confidence in the accuracy of the result, or an understanding of where and how the system made an error. An election system forensics examination may also lead to information that can be used to correct the errors in a manner that will allow the system to produce results that accurately reflect the voters' ballot choices.

13. A post-election forensics examination requires collecting and analyzing several types of data:

- a. Records of any indication of failures such as an error message on a screen, and as much information about what happened and at what stage in the process it happened;
- b. Records of any data relevant to the e-voting system, such as how physical access to the system was controlled;
- c. Vote totals, electronic ballots, and any voter-verified paper audit trails or paper ballots; and
- d. Source code and build procedures and environments, so the analysts can examine the software and, if necessary, regenerate it.

14. The steps in a forensic examination or audit can vary, depending on circumstances and what data is available. Basically, the analysts correlate the data they have, looking for inconsistencies and anomalies. They also (possibly concurrently) analyze the source code to determine if there are programming errors or inconsistencies that might cause problems, and if found determine whether those problems either occurred (ideally) or could have occurred. They can then attempt to reproduce those problems on the actual voting systems used in the election.

15. As an example, one of the first things the team would look at is the components of the software, how they interact, what their limits are, and what happens if those limits are

exceeded. This would, for example, answer the questions posed above about what happens if the Microsoft Access database limits are exceeded and large numbers are added together.

16. Assuring appropriate technical qualifications for team members is critical to the success of the forensic examination. Members of the team will need to analyze complex software, and how different integral components interact, often on a very tight timetable. Thus, some members of the team must be experts in computer security and forensic analysis. Further, at least one team member should have experience in analyzing e-voting systems, because that experience is invaluable to the entire team's efficiency. Perhaps most critical is a team member who has expertise and experience in how elections in the jurisdiction are administered, and the procedures normally used.

17. With the results of a forensic examination, the election officials, and the public, will have more confidence in both the results and the systems used in the election. It will show the concern and care that election officials have about the accuracy of the results of an election that they run. Even if problems were to be found, the fact that the public authorities have not hidden them but have sought to investigate promptly and publicly will increase the trust and confidence of voters in the way an election is conducted and the results verified.

Conclusion

18. My findings and experience in analyzing e-voting systems demonstrates that there is a considerable question as to whether these systems are accurate and robust enough for use in general elections. We found that the ones used in California were not, as of the summer of 2007, despite being certified to meet the requisite e-voting standards. Only a close evaluation of the source code and the voting systems will reveal whether Pennsylvania's voting systems were compromised with these same or similar vulnerabilities.

19. I understand that questions have been raised about the accuracy of the results of the election. A forensic examination, in which the examiners could analyze the components of the system, the data gathered during the election, and the results would help answer these questions. A manual recount where paper ballots are used would also answer these questions in those jurisdictions. These procedures would establish a high level of confidence in the results of the election.

20. Given the questions raised about the election results, I believe that these measures are appropriate and fully warranted.


This affidavit was executed on the 2nd day of December, 2016, in Davis, California.

Matthew A Bishop

Matthew A. Bishop

Sworn before me this 2nd day of December, 2016.

*Please See California Jurat below.
GC 12/02/16*

 _____
Notary Public

My Commission expires: _____

A notary public or other officer completing this certificate verifies only the identity of the individual who signed the document to which this certificate is attached, and not the truthfulness, accuracy, or validity of that document.

State of California

County of Yolo

Subscribed and sworn to (or affirmed) before me on this 2nd day

of December, 2016, by Matthew A. Bishop

N/A, proved to me on the basis of satisfactory evidence to be the person(s) who appeared before me.

Signature  (Seal)

